EXHIBIT C

From the MIT Technology Review
April 4, 2014

http://www.technologyreview.com/view/526161/the-troubling-holes-in-mtgoxs-account-of-how-it-lost-600-million-in-bitcoins/

The Troubling Holes in MtGox's Account of How It Lost $600 Million in Bitcoins

Computer scientists, who have been monitoring the Bitcoin network since January 2013, cast doubt on MtGox's claim that its bitcoins were stolen by hackers.

On February 10, a Bitcoin exchange called MtGox announced it had lost some 850,000 bitcoins, of which 750,000 belonged to its customers. At the time, bitcoins were trading at $827 apiece, making the value of the loss equivalent to $620 million.

That's a significant shortfall by anyone's standards. But MtGox had an explanation. In a press release on that day, it announced it had been the victim of a fraud in which the bitcoins had been stolen by hackers.

The fraud, said the company, was a result of a problem known as a transaction malleability bug. This allows malicious users to transfer bitcoins into their

accounts while making MtGox think the transfer had failed. Consequently, MtGox repeated these transactions so that the total amount was transferred twice.

Today, Christian Decker and Roger Wattenhofer at the Swiss Federal Institute of Technology in Zurich cast doubt on this version of events. These guys have been monitoring bitcoin transactions since January 2013 in a way that allows them to detect malleability bug transactions. And they say that the total number of fraudulent transfers in that time is several orders of magnitude smaller than MtGox claims.

Decker and Wattenhofer began monitoring the Bitcoin network in January 2013. They recorded all transactions, as well as those that were blocked, by connecting to around 1000 nodes in the Bitcoin network. That's about 20 percent of the total.

When a transaction is made, the details spread through the network telling other nodes who now owns the bitcoins. When the transaction fails, news of this also spreads so that everyone's records can be updated.

The malleability bug allows a malicious user to secretly change these details so that the original sender thinks the transaction has been blocked while everyone else thinks it has succeeded. But Decker and Wattenhofer were able to record when this happened by looking for instances when the same transactions differed in the relevant details.

During the year or so that they have been gathering their data, Decker and Wattenhofer have observed a total of 302,000 bitcoins involved in malleability attacks. However, the vast majority of these occurred after MtGox's February 10 press release, and appear to be copycat attacks triggered by the news that they could be successful. These, presumably, cannot have involved MtGox because it had prevented its customers from accessing their accounts by then.

The numbers involving MtGox before then were far fewer. "Only 1,811 bitcoins were in attacks before MtGox stopped users from withdrawing bitcoins," say Decker and Wattenhofer.

What's more, some 75 percent of these attacks were ineffective. "As such, barely 386 bitcoins could have been stolen using malleability attacks from MtGox or from other businesses," they conclude. This is three orders of magnitude less than the number MtGox claims.

That's an interesting study that leaves a gaping hole in MtGox's account of what happened. "Even if all of these attacks were targeted against MtGox, MtGox needs to explain the whereabouts of 849,600 bitcoins," say Decker and Wattenhofer.

A curious corollary to this story is that a couple of weeks ago, MtGox announced that it had found 200,000 Bitcoins on an old hard drive. Those ones, at least, had not been stolen. The whereabouts of the rest is still unknown

This is a spectacular collapse. In 2013, MtGox was handling 70 percent of all bitcoin transactions. Today, it has suspended trading, closed its exchange and filed for bankruptcy protection.

We emailed MtGox for comment but haven't heard back. Clearly, there is more to this story to come.

Ref: http://arxiv.org/abs/1403.6676: Bitcoin Transaction Malleability and MtGox